As SD-WAN continues to be adopted for internet-based WAN architectures, associated security architectures continue to evolve as well. This research offers security and risk management leaders guidance on where and how to secure these internet connections.

Overview

Key Findings

- As SD-WAN is enabling direct internet access to branch offices, security and risk management leaders are challenged to find the optimum security architecture to fulfill their security needs.

- Converged secure access service edge (SASE) offerings are available that combine SD-WAN with local and cloud-based security services; however, there are gaps in terms of services functionality across providers.

- Cloud-delivered security is available from a range of different providers, which highlights the need to discern how to best integrate with evolving WAN architectures and how they intersect with security requirements.

Recommendations

Security and risk management leaders with responsibility to secure branch office internet connectivity should:

- Simplify branch office internet access security by using hosted or cloud-based security where possible.

- Evaluate the pros and cons of using an integrated single vendor/provider versus multiple best-of-breed vendors for both networking and security.
Integrate SASE with a global enhanced internet backbone service that optimizes connectivity to applications like SaaS-delivered business-critical applications.

**Strategic Planning Assumption(s)**

By 2024, at least 60% of global SASE services will be offered integrated with an optimized internet backbone to ensure performance of global internet WAN connectivity, up from less than 10% year-end 2020.

By year-end 2024, at least 10 vendors will offer an integrated SASE solution rather than multiple separate component parts, as is the case today.

**Introduction**

The evolution of the enterprise WAN is seeing network leaders shifting to utilize the internet for all their connectivity needs for the branch offices, as illustrated in figure 1. This can pose a challenge for security and risk management leaders that are investigating measures to reduce the number of appliances and are increasingly moving security out of appliance-based deployments to support application performance for branch offices with direct internet connectivity.

Many security leaders have established strategies toward SASE architectures. While SD-WAN security is a component of SASE, there are security leaders that need tactical SD-WAN security solutions, either instead of SASE or as part of their migration toward SASE.

This research describes the options to secure SD-WAN connectivity, and how security and risk management leaders in collaboration with network leaders can select a solution optimum to both networking and security needs.
SD-WAN emerged as a simple way to create a hybrid WAN to move traffic away from the Multiprotocol Label Switching (MPLS) WAN to the internet. The most simple use case is enterprise sites connecting to a data center in a basic “hub and spoke” topology, while concurrently allowing for better management of traffic with software-defined methods. This architecture often has no intent of supporting direct internet access from these sites. It merely establishes secure tunnels from each site to a data center, either in hybrid WAN of internet and MPLS or only internet in order to drive down WAN cost.

Analysis

Simplify Branch Office Internet Access Security by Using Cloud-Based Security

Increased internet connectivity is expanding attack surfaces.
The goal should be that traffic destined to a place on the internet is routed as directly as possible and not tromboning back to the head office to then exit to the internet. Security is often via basic Layer 3/4 security features supported by most SD-WAN products, as listed in Note 1. This type of WAN design is typically targeted at retail outlet connectivity such as bank outlets, ATMs, gambling sites, clothing chains or auto dealerships, which have large numbers of smaller branches.

Figure 2 illustrates SD-WAN design using embedded security.

**Figure 2. SD-WAN Design Using Embedded Security**

---

**Complement SD-WAN With Cloud-Based Security Services**

The majority of SD-WAN vendors have augmented their solutions with the ability to service-chain with third-party cloud-delivered security solutions like secure web gateway (SWG) and cloud access security brokers (CASBs). This use case should be considered for smaller branch offices where staff is only using few, if any, “intranet” types of applications and the end-user security requirements are entirely focused on securing traffic on the HTTP/HTTPS protocols. In recent years, the CASB (see Magic Quadrant for Cloud Access Security Brokers) and secure web gateway (see Magic Quadrant for Secure Web Gateways) markets have been converging, further reducing security vendor selection bifurcation (see Select the Right Strategy for Securing Web Access).
The benefit of these cloud-delivered security solutions is that, regardless of location of the branch and/or user, their use of globally distributed point of presence (POP) can ensure that both availability and performance can be maintained while not sacrificing security efficacy. Security and risk management leaders should take these measures into account in evaluating vendors’ claims since they are differentiating features for security vendors today. Ask the security providers for specific latency commitments. Figure 3 illustrates SD-WAN design using service chaining with cloud-delivered security solutions.

**Figure 3. SD-WAN Design Using Service Chaining With Cloud-Delivered Security Solutions**

Consider SD-WAN with an on-site branch firewall only when necessary.
An enterprise firewall, either embedded in the SD-WAN or a stand-alone firewall, is typically used to secure branch offices when there are specific needs. Examples include consuming a complicated mix of internet and data center (aka intranet) services like collaboration (voice/video), thick client types of applications, and applications requiring sophisticated filtering of access to the internet that includes user/application visibility and enforcement, URL filtering, and locally based anti-malware capabilities. Additionally, branch firewalls allow for intra-branch traffic segmentation use cases that cannot be readily delivered by the cloud. This is a role better filled by enterprise firewalls either as small branch appliances or functionality delivered from the cloud, where possible. From a network perspective, there are multiple SD-WAN solutions that support enterprise firewall functionality (see Note 2). Historically, security and risk management leaders have chosen a separate vendor from the WAN because there were different vendors’ best-of-breed solutions (e.g., Versive and Checkpoint) or if there were different solutions from the same vendor (e.g., Cisco ISR and Meraki). This is changing in that many firewall vendors have been adding or at least messaging on being able to deliver WAN features alongside their existing network security feature set.

The belief that the firewall is separate from the router still persists. It is still a valid option because it supports best of breed for networking and security and also facilitates separation of duties and different vendor skill sets in an IT team. For example, the networking team could have good domain expertise in Juniper for their network, but not Checkpoint. Likewise, the security team might have Fortinet firewalls, but not know HP Networking.

Security and risk management leaders today have a different choice for their digital business. They can move to an SASE architecture that is more agile and easier to manage, while sacrificing nothing in terms of security efficacy. Figure 4 illustrates SD-WAN with on-site SD-WAN and an enterprise firewall.
Enterprises that need a branch firewall, as described in the previous use case, are increasingly looking toward providers that offer firewall as a-service (FWaaS) or SASE, which is following the security industry trend for cloud-delivered security. The advantage is avoiding deploying complex functionality in branch offices and, instead, using cloud-scalable services located off network and service-chain with SD-WAN in each branch office. This also reduces the number of physical appliances that have to be deployed and maintained in branch offices.

Many options are available from security vendors, over-the-top providers and network service providers (see Note 3). Examples are vendors offering services based on their own integrated products, while network and carrier service providers typically offer a range of SD-WAN and security products packaged together based on required outcomes.
Security and risk management leaders seeking these services should evaluate how they can integrate with existing operations for the best management of policies and ensure no reduction in security efficacy. These cloud-delivered security services often use a fabric of POPs that are scalable and have SLA guarantees around service availability and network latency. It should also be possible to terminate the SD-WAN session at the cloud security providers’ POPs or, if direct-to-cloud is preferred, have sessions directed to the data center of the cloud service provider. Figure 5 illustrates SD-WAN design with FWaaS.

**Figure 5. SD-WAN Design With Firewall as a Service**

Traditional security capabilities are now available as-a-service from the cloud, while concurrently there is also a blurring of networking and security with the convergence trend of SASE disrupting both pure play networking and security. With that today we now see SD-WAN being offered with more security features, and likewise, cloud-delivered security providers delivering more capable SD-WAN like features. In fact, in some cases, SASE Security services and SD-WAN are increasingly hard to pull apart.

**Evaluate Using a Single Vendor/Provider Versus Multiple Best-of-Breed Vendors for Both Networking and Security**
As enterprises move to use internet connectivity for their branch offices, and remote and mobile workers, as well as various endpoint devices, the task of security is now a business issue that needs to be addressed architecturally. Traditional security approaches are based on defining policies with broad permissions enforced at the traditional network perimeter. Though functional, these approaches typically are not scalable, require more administrative overhead and cost to manage, and, importantly, grant too much trust by default. This is where zero-trust principles delivered from the cloud are proving their worth, with enterprises increasingly upgrading to new providers or consuming this model of access from their existing provider(s), when available.

A further convergence trend that has emerged is integration of SD-WAN with cloud-delivered network security into SASE services. This means that branch office SD-WAN appliances, SD-WAN soft agents and SD-WAN gateways are fully integrated with the security functionality.

Figure 6 illustrates WAN design incorporating SASE.
Gartner believes that there are currently around eight vendors (Palo Alto Networks, Cisco, Versa, Cato, Forcepoint, Citrix, Open Systems and Fortinet) that can deliver SASE solutions with all functions listed in Figure 6 (i.e., SD-WAN and a set of associated local and cloud-based security services [SWG, FWaaS, ZTNA, CASB]) (see Hype Cycle for Cloud Security, 2020). However, while these vendors support all functional groups, they are not equally strong within all of these functions. This means that enterprises that traditionally have been sourcing best-of-breed products need to evaluate the pros and cons of using a single vendor/provider versus multiple best-of-breed vendors for both networking and security. Using a single vendor with a fully integrated SASE solution offers operational advantage, while a best-of-breed provider requires more time and skills to integrate and manage. If multiple vendors are used, enterprises should require explicit partnerships with strong integration and technical support.
Integrate SASE With a Global Enhanced Internet Backbone Service for Additional Simplification of Service Sourcing

The need for SASE is driven partly by a need for identity-based policies to strengthen security and partly for converged solutions that can make it easier to maintain policies. This is already evident by the growing desire to source all cloud-based security from one vendor. For example, by 2024, 30% of enterprises will adopt cloud-delivered SWG, CASB, ZTNA and branch office FWaaS capabilities from the same vendor, up from less than 5% in 2020 (see 2021 Strategic Roadmap for SASE Convergence). The convergence of these security functions with SD-WAN into emerging SASE solutions will further simplify deployment and policy management. However, there are further opportunities for improvements.

Enterprises with strong strategies toward internet as the preferred transport should integrate their SASE services with an enhanced internet backbone for three reasons:

- The end-to-end application performance will become predictable.
- By integrating SD-WAN with such a backbone, it is possible to better match application performance policies with the backbone path topology.
- By integrating security with the backbone, it is possible to manage cloud service access in a more efficient manner.

This new WAN architecture will thus consist of a service edge distributed around the backbone and offer a flexible interconnect platform for all end users, offices, partners and applications. Figure 7 illustrates SASE integrated with an enhanced internet backbone service.
Preference SD-Wan providers that have an ecosystem of supported security vendors cloud delivered services available for integration with the WAN where you do not run a fully converged architecture.

**Evidence**

Inquiry trends over the last 12 months show that SD-WAN, internet and SD-WAN security remain in the top five of more than 100 inquiry topic areas. Typically, these discussions include security and evolving security architectures.

The data collected from our WAN edge infrastructure Critical Capabilities and Magic Quadrant research shows that eight out of 20 surveyed SD-WAN vendors support enterprise firewall capabilities, and four of these are rated in the Leaders quadrant of the Magic Quadrant for WAN Edge Infrastructure.
The data collected from our network services Critical Capabilities and Magic Quadrant research shows that all surveyed service providers continue to deploy more network hubs in more countries. They also expand their selection of SD-WAN vendors and security vendors for their virtualized services.

**Note 1: Basic Security Features**

Many SD-WAN products only support basic security features, some Layer 3 and others Layer 4, but do not support more advanced controls, which is generally required for strong security solutions (see *Critical Capabilities for WAN Edge Infrastructure*). Instead, they typically support similar security features as in traditional routers:

- IPsec-based IPVPN
- Basic stateful firewall capabilities such as policy-based filtering and blocking of applications, ports and IP addresses (access control list)
- Basic denial of service (DOS) prevention
- Network address translation

**Note 2: SD-WAN Vendors With Support of Embedded Enterprise FW**

Most SD-WAN vendors only support basic security features, but a few vendors support both SD-WAN and enterprise FW. Examples include:

- Barracuda
- Cato
- Cisco
- Forcepoint
- Fortinet
- Palo Alto
- Juniper
- Versa
Note 3: Evolving Options for Cloud-Based Security

Besides traditional on-premises secure gateway services, which currently only constitute around 30% of SWG deployments, there are several network security options available in the market, such as dedicated managed services.

Dedicated Managed Services

Network service providers have been deploying network nodes from which they offer a range of virtual network functionality as dedicated managed services. In many cases, providers offer a range of security options and vendors, and enable integration with existing enterprise operational systems. Security providers like ZScaler and Akamai have also been building out an extensive cloud edge fabric that facilitates various SD-WAN and/or complementary over-the-top (OTT) capabilities that directly support SD-WAN.

Cloud-Delivered Security Services

Security providers now offer cloud-delivered security services that are largely similar to their on-premises offerings. Vendors such as Symantec, McAfee, Palo Alto, Fortinet and Forcepoint have a broad range of security capabilities that meet the stricter security efficacy requirements security teams demand. Also, enterprises continue to adopt the pure-play cloud-delivered security providers like ZScaler.

Enhanced Internet Services

Enhanced internet service providers such as Aryaka, Cato and NetFoundry offer security services from their network hubs in addition to other network functions.

Enterprise-Managed Hosted Security

Enterprises seeking maximum flexibility can deploy their own solution in hosting facilities, either in-house managed or provider-managed, or in-cloud service providers. These types of deployments are becoming only slightly easier for end users to consume. Some providers such as Equinix, Megaport and PCCW make virtual network functionality available for on-demand deployments that may ease this burden to a degree. This method tends to be relatively complicated and is a path not chosen by the majority of Gartner clients today.

Recommended by the Authors
Some documents may not be available as part of your current Gartner subscription.

Critical Capabilities for WAN Edge Infrastructure

Magic Quadrant for WAN Edge Infrastructure

Magic Quadrant for Enterprise Network Firewalls

Forecast: Enterprise Communications Services, Worldwide, 2016-2022, 4Q18 Update

Market Guide for Zero Trust Network Access

2021 Strategic Roadmap for SASE Convergence

Market Guide for Network Access Control

Magic Quadrant for Secure Web Gateways

Select the Right Strategy for Securing Web Access

© 2021 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."